

ULTRA AND THE WALKER CASE

Captain Esmond D. Smith, Jr., USN

Modern military services, particularly navies, depend heavily on secure radio communications in all aspects of their operations. To protect these communications, messages are enciphered using cryptographic systems so that only holders of the same systems can decipher the messages. If, however, an adversary develops the capability to decipher these communications and the users are unaware of this capability, the adversary has acquired an intelligence source of unparalleled accuracy and utility. In the event of war, such a source could mean the difference between defeat and victory.

British and American cryptological successes before and during World War I and the American successes against Japanese naval codes in World War II are just two examples of the significance of this intelligence source. The British exploitation of German naval communications during the war in the Atlantic in World War II provides an even more pointed example of the war-winning utility of this source. Unfortunately, these and other similar examples are not merely of historic interest. Through the recent activities of the John Walker spy ring, the Soviet Union acquired the capability to decipher secure communications of the US Navy from 1967 to 1984.

One common element in the success of the British in deciphering German naval communications during World War II and the recent success of the Soviets in deciphering US Navy communications was that in both cases the users of these communications remained unaware that their messages were being compromised.

Ultra and the Atlantic War

During World War II, British cryptanalytic efforts, in conjunction with other forms of intelligence, enabled the Allies to read German naval and other military message traffic. The Germans were scoring similar successes against British communications. The British, however, deduced that their naval communications had been compromised, and they were able to defeat the German cryptologic effort by introducing a new, improved cipher system. The Germans, on the other hand, failed to discover that their naval communications were being exploited by the British through the end of the war.

Ultra was the codeword for special intelligence derived from successful British efforts to break the codes used to transmit German military radio traffic. These military messages were machine-encrypted by a cryptographic device called the Enigma machine. All three German services used the machine, although each used its own type of "key"—the rotor order, ring settings, plugboard connections and ground settings, which were changed frequently. In addition, each service used different key settings for each communications

network. In some networks, messages were double-enciphered using two key settings, making them extremely difficult to break using cryptanalytic methods. The German Navy also strove for even greater security by the use of four-letter code groups, keyed to code books, that were placed in the text of some messages before encryption.¹ Thus, the German military, and particularly the German Navy, had good cause to believe that its communications were secure.

The British code-breaking establishment at Bletchley Park, however, had obtained an Engima machine from the Poles in August 1939, along with instructions for breaking the Army and Air Force keys.² At various times throughout the war, the British acquired additional pieces of Enigma equipment, codes, and key settings from captured German ships and submarines. This material greatly assisted the cryptanalytic attack by Bletchley Park, and, by the spring of 1941, the Allies began to obtain invaluable intelligence from German naval operational message traffic.

To protect Ultra, knowledge of the source was limited to a handful of senior naval officers, and any operations based on Ultra information had to have a plausible cover story. Ultra messages were themselves enciphered using a one-time pad, providing total security, and special storage and accounting procedures for Ultra material were rigidly enforced.³

As the volume and timeliness of the Ultra material improved in late 1941, it became possible to make tactical use of the information derived from this source. This was particularly important in the war in the Atlantic, where Ultra information on the location and situations of German U-boats was used to reroute convoys.

This and other operational uses inevitably resulted in raising the Germans' suspicions about their security. These concerns generally focused on Allied espionage networks rather than on the security of German communications. Several times during the war, the Germans did suspect that disastrous changes in their fortunes might have been due to communications vulnerabilities, and they made a few checks and minor changes. Even after the war was over, however, Commander of U-boats Admiral Doenitz did not know that the British had been exploiting his message traffic.

No Questions Asked

Why, in the face of considerable evidence of Allied foreknowledge about German U-boat operations, was the security of German naval communications never seriously questioned? There appear to be several related answers to this question:

- The difficulties that the German cryptologic services had with British codes in the early days of the war made them confident that the Allies would have similar problems with their own ciphers.

- There were often other possible explanations for Allied actions, including air reconnaissance, the use of radar and high-frequency directionfinding and Allied espionage activity. This was generally supported by the care with which the British tried to use Ultra information operationally.

- An implicit understanding of the logistic and other difficulties in developing and fielding an entirely new cipher system to all German military users during wartime.

- The German organization that investigated Doenitz's security concerns—the Naval Intelligence Service—was the same service that was responsible for the cipher systems used in German naval communications. Thus, there probably was an institutional bias against the possibility that the ciphers were being broken.

- A psychological tendency to discourage suspicions of the Engima system. As one author states, "They believed it was absolutely secure because they wanted to believe it was secure."⁴

These postulated reasons are mutually reinforcing, and they tend to support the last one. In the final account, it may be the most important. It also may have been the case in a more recent example.

The Walker Spy Ring

In many ways, the John Walker espionage case is completely different from the British cryptologic effort during World War II. Both, however, resulted in the compromise and exploitation of an adversary's secure communications. The well-documented Walker case needs only a brief description here.

In May 1985, following a long and often convoluted espionage investigation, the FBI arrested John Walker and the three other members of his spy ring—his son, Michael Walker; his brother, Arthur Walker; and a friend, Jerry Whitworth. All are now serving sentences in federal prisons.

John Walker and Whitworth were the ring's key members. Both had served in the US Navy as communications specialists and had access to US military cryptographic material and information. John Walker sold the Soviets this material from at least 1967 until his retirement from the Navy in 1976; Whitworth's involvement possibly dates from the time he was recruited by Walker in 1971 until his own retirement from the Navy in 1984.

Immediately following the arrest of these individuals, the government began an investigation into the damage they had caused to national security interests. The US Navy initially considered the potential compromise damaging but manageable. In assessing the impact of the Walker-Whitworth betrayal a month after their arrest, Admiral James D. Watkins, the Chief of Naval Operations, declared that the Navy had the problem "bounded and can leave it in the dust behind us . . . We believe that we are on the downside of the problem . . ."⁵ This sanguine view did not last long, however. In July 1985, a high-ranking Soviet KGB defector, Vitaly Yurchenko, told his FBI debriefers that "the information delivered by Walker enabled the KGB to decipher over a million messages."⁶ This number probably understates by a wide margin the actual number available to Soviet interceptors and vulnerable to compromise. While there is no way of knowing what specific messages were read by the Soviets, former Director of Naval Intelligence Rear Admiral William Studeman has testified that they probably included classified messages regarding

naval ship locations and operations, naval intelligence data and activities, and naval plans and procedures.⁷ In most cases, the tactical value of the messages provided by the spy ring probably was questionable, however, because many of the messages probably were months old by the time the Soviets deciphered them. It seems likely that the most serious damage done by the ring's information lay in what it taught the Soviet Navy about its technological and doctrinal inferiority and about where the next generation of American weapons and sensors were going in terms of capabilities.

Occasionally, there were reasons to believe that classified operations were being compromised in some way. But if these were investigated, the source of the compromise was usually attributed to poor operational security—discussions in public places that could have been overheard and logistic or other operational patterns that Soviet analysts could have pieced together—rather than to insecure communications. These explanations did not satisfy everyone, however. Suspicions grew as Soviet intelligence collection ships began to show up routinely in exactly the right places and times to monitor our exercises or weapons tests, as the Soviets reacted in unexpectedly low-key ways to our naval operations near their coasts, and as the quality of Soviet ships, submarines and aircraft began to improve much faster than our estimates had anticipated. Rich Haver, the deputy director of Naval Intelligence and one of the Navy's most experienced analysts of the Soviet Navy, periodically voiced his concern. One source reports that, beginning in the early 1970s, Haver periodically saw signs that "something was wrong," because the Soviets knew things they should not have known. Privately, he sometimes wondered about the security of US communications, but he had no proof. Discovery of the Walker-Whitworth espionage ring suddenly made everything clear.⁸

The fact that our communications were being exploited from at least 1967 onwards by the Soviets may account for certain US military operational "failures." The abortive raid on the Son Tay prisoner of war camp in 1969 in North Vietnam provides one such example. The camp was suddenly evacuated by the Vietnamese several weeks before the raid took place. Had the Soviets learned about the raid from our communications and told their Vietnamese allies about it in advance? On the other hand, the Soviets might have been reluctant to risk such a valuable source just to provide tactical support to the Vietnamese. Hanoi may have been alerted to the raid by its own intelligence sources and analysis.

Security Shortcomings

When the details of the British use of Ultra in World War II were declassified and released in 1974, the entire war, particularly the conflict in the Atlantic, had to be reexamined. When and if specific compromises resulting from the Walker case are publicly released, recent history will also have to be reviewed. Such a review could disclose that the security of our naval communications was never seriously questioned for the following reasons:

- The National Security Agency (NSA), the government agency responsible for communications security (comsec), considered that most of the cryptographic systems in fleetwide use were adequately secure from foreign cryptologic attack (which they probably were).

- The procedures established by NSA for controlling and handling cryptographic equipment and keying materials, if universally and uniformly followed, would have provided adequate security of this material from theft or espionage. In the same way, established procedures for background investigations should have ensured the integrity of the individuals with access to cryptographic materials. Obviously, neither of these procedures were followed in the case of the Walker spy ring.

- As was the case with the German Intelligence Service in World War II, NSA may have had an institutional bias against the possibility that the systems and procedures that it had implemented were being exploited. Investigations into suspected security leaks would be focused on exhausting all other possible sources of the leak before the security of crypto-covered communications was questioned.

- In many cases, there *were* other possible sources of these leaks, ranging from discussions on insecure telephones to operational security indicators. These could have been used by foreign intelligence analysts to gain foreknowledge of US naval operations.

- To avoid arousing suspicion, the Soviets, like the British in World War II, are likely to have made careful use of the intelligence gained from US communications. Information about the Walker spy ring probably was tightly compartmented within the highest levels of the Soviet intelligence establishment. (Yurchenko was only "briefed in" on the Walker case by the KGB so that he could conduct an investigation of how Walker was caught.)

- The cost and logistic difficulties involved in changing US naval communications cryptographic systems worldwide would be staggering. Such a move could not be done without hard evidence that these communications systems were being exploited, which the Soviets could have gone to great lengths to avoid providing. With Walker and Whitworth operating *inside* the naval communications organization, such changes would have been immediately passed on to the Soviets, anyway. Nonetheless, the immense costs of such a change would tend to reinforce a belief that our communications were secure.

In any case, it appears that we shared many of the reasons that the Germans had for believing in the security of their naval communications. The obverse, that our communications were not secure, was too damaging to contemplate. Quoting Rear Admiral Studeman again, "... virtually all the information required to plan, operate, command, maintain, modernize, repair, replenish, warn, inform and control the military forces of all the services and our allies is exchanged electrically via communications systems, most of which are considered secure by virtue of their cryptographic cover." ⁹

More Safeguards Needed

There is no easy solution to this crucial problem. New procedures and systems are likely to ensure the security of our naval communications over the short term. The Soviets have proven to be patient and cunning adversaries, however, and even now they could be attacking our communications systems

using high-speed computers or recruiting the next generation of spies to provide key material.

Is there anything that we can learn from these two cases to augment our technical efforts for safeguarding our secure communications? The comsec problem involves a number of different disciplines, including physical security, comsec procedures, cryptographic systems, foreign collection systems, integrity of personnel, and espionage. Thus, any approach to the problem has to be truly multidisciplined.

- A permanent Department of Defense committee comprised of members from the various government intelligence agencies should be established on a continuing basis to investigate and appraise the security of US Government communications, using all available sources of intelligence and other information. This joint committee should act as a clearing-house in following up on anomalous or unexplained foreign activity that might be related to comsec.

- Existing comsec and personnel procedures should be strictly adhered to by all government agencies and branches of the armed services. Command responsibility for violations of these procedures should be an explicit element of these procedures.

- Current procedures should be reexamined periodically to determine their feasibility and effectiveness. Where possible, security-related procedures should be simplified and streamlined to ensure that they are universally understood and implemented.

- Security awareness programs should be expanded in order to educate our personnel regarding the foreign espionage threat and possible indicators of espionage activity.

- Consideration should be given to the use of a "security minimize," which would caution commanders from using regular secure communications in areas or during periods of known foreign electronic collection activities.

- For particularly sensitive message traffic, the use of nonelectrical means of communications, including the use of officer couriers, fiber-optic landlines and other high-technology systems, should be investigated.

None of these suggestions will ensure the security of our communications, because all of them depend on the weakest link, human beings, to implement them. The easiest way to exploit secure communications is to recruit an agent within the system who either copies the messages or provides our adversaries with the ability to copy them themselves. We may not be able to stop such espionage activity, but we can certainly make it harder for our enemies to obtain sensitive information.

The real lesson that these two cases provide is that comsec cannot be taken for granted. A final quote from Rear Admiral Studeman sums up the problem: "History is replete with examples of the benefits and risks associated with comsec made vulnerable by espionage or otherwise penetrated for the benefit of one side or another. Such vulnerabilities sustained over time have altered the course of history and can do so again in the future."¹⁰

NOTES

1. Ralph Erskine, "Naval Enigma: The Breaking of Heimisch and Triton." *Intelligence and National Security* Spring, 1988 pps. 162-163.
2. Erskine, p. 163.
3. John Winton, *Ultra at Sea* p. 4.
4. Winton, p. 104.
5. Thomas B. Allen and Norman Polmar, *Merchants of Treason*, (New York: Delacorte Press, 1988) pps. 262-263.
6. U.S. Congress, Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Foreign Missions Act and Espionage Activities in the United States*, Hearings, (Washington: U. S. Govt. Print. Off., 1986), p. 103.
7. U. S. Congress, pps. 99-100.
8. John Barron, *Breaking the Ring*, (Boston: Houghton Mifflin Company, 1987) pps. 209-210.
9. U.S. Congress, p. 97.
10. U.S. Congress, p. 99.